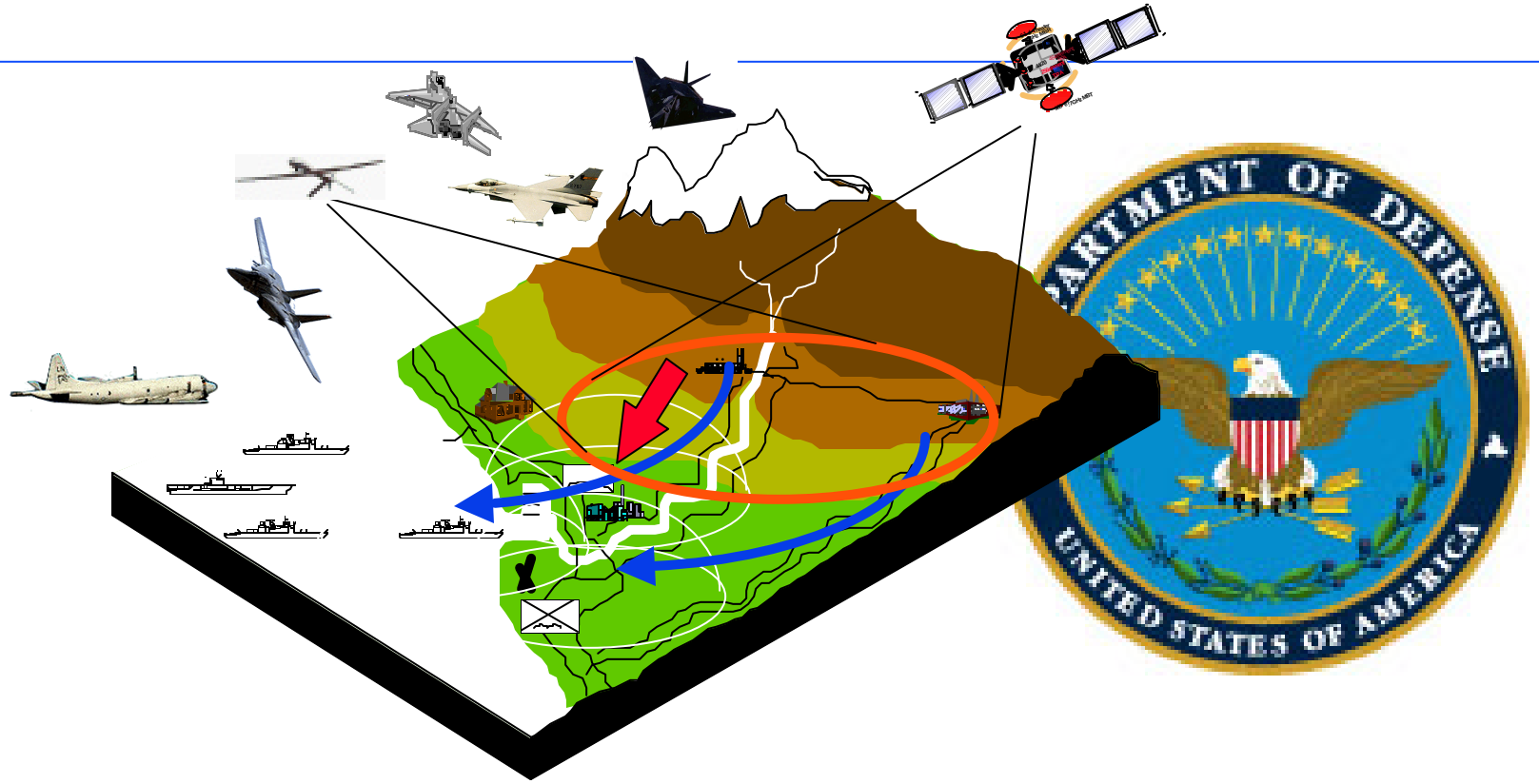


C4ISTAR and the Global Information Grid

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
23SEP2001	N/A	25SEP2001 - 27SEP2001

Title and Subtitle C4ISTAR and the Global Information Grid	**Contract Number**
	Grant Number
	Program Element Number
Author(s) Hynes, Rosanne	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) US Department of Defense	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es) EOARD PSC 802 BOX 14 FPO 09499-0014	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes
See Also ADM001419 for whole conference on CD-ROM. These papers are from the Harnessing Advanced Technology for C4ISTAR, The Second Annual Advanced Technology Conference, held 25-27 September 2001 at The Great Malvern Theatre Complex., The original document contains color images.

Abstract

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU

Number of Pages
30

Operational Realities

- Reduced force size
- Bandwidth intensive
- Higher mobility
- Asymmetric threats
- Wide variety of missions
- Rapid force projection
- Higher operations tempo
- Joint and Coalition Warfare

- Dynamic planning and redirection of assets
- Support of ad hoc military/civil structures
- Multidimensional awareness and assessment
- Split base/Reachback Operations
- Increased threats to networks

A Future which is Filled with Both Promise and Peril

Summary of Emerging Evidence

Task Force XXI Advanced Warfighting Experiment

Faster, precision maneuver for lethal, evasive engagement of enemy ground force based on shared battlesspace awareness & tactical synchronization

Fleet Battle Experiment (FBE) Delta

Internetting of AEGIS and Firefinder radars for counter-battery fires.
Aggressive prosecution of Special Operations Forces (SOF) threat based on shared awareness and rapid, self-synchronized engagement

Expeditionary Force Experiment (EFX)‘98

Joint Forces Air Component Commander (JFACC) Enroute
Bombers linked into tactical info grid for beyond-line-of-sight retargeting
Reduced Joint Air Operations Center (JOAC) forward footprint

Operation Allied Force

Reduced targeting timelines with Distributed Common Ground Systems

McCarthy Panel

"No capability is more important than situational knowledge shared among all elements of the joint force (much greater emphasis on "shared", "all" and "joint"). This shared situational knowledge provides the foundation for new capabilities"

McCarthy Panel Press Briefing, 12 June 2001

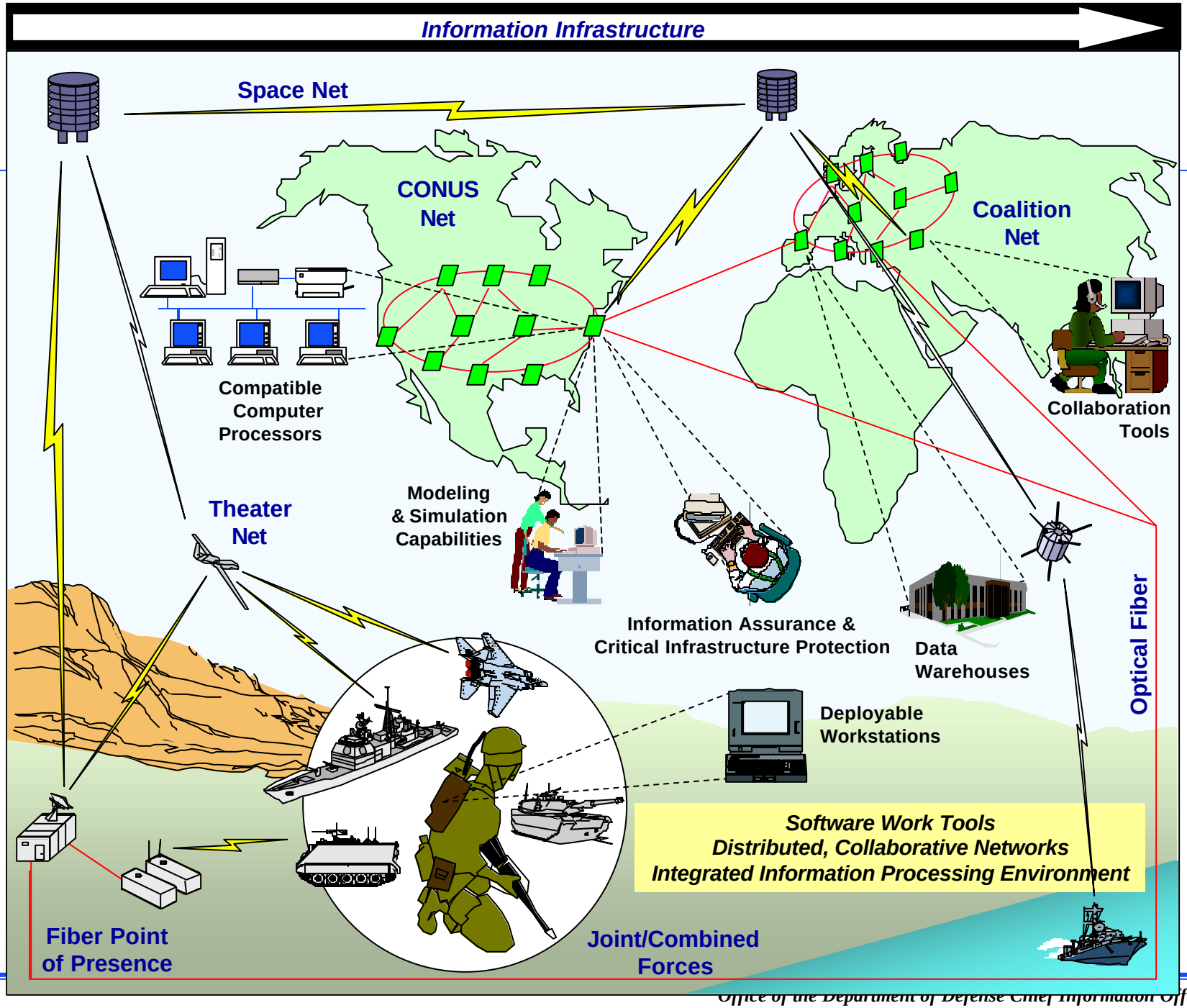
Some High Interests Programs

- Distributed Common Ground Systems
- ISR Battle Manager - Asset Visibility Tools
- Integrated Collection Management
- Collaborative Analysis Tools
- Geospatial Foundation/Targeting Databases
- Unmanned Aerial Vehicles
  - accelerate SIGINT capable Global Hawk
  - accelerate development of stealth
- Joint Deployable Command and Control

SecDef -- Two truly transforming things

"The two truly transforming things, conceivably, might be in information technology and information operation and networking and connecting things in ways that they function totally differently than they had previously. And if that's possible, what I just said, that possibly the single-most transforming thing in our force will not be a weapon system, but a set of interconnections and a substantially enhanced capability because of that awareness."

Extracted from SecDef Town Hall Meeting, 9 Aug 2001


Information Infrastructure
Space Net
CONUS Net
Coalition Net
Compatible Computer Processors
Collaboration Tools
Theater Net
Modeling & Simulation Capabilities
Information Assurance & Critical Infrastructure Protection
Data Warehouses
Optical Fiber
Deployable Workstations
Software Work Tools
Distributed, Collaborative Networks
Integrated Information Processing Environment
Fiber Point of Presence
Joint/Combined Forces

Enterprise Operating Models

Federated Operations

Enterprise Value derives from mostly functional processes, some operating in a "just in time" manner. Cross functional contributions to enterprise value are relatively limited.

Lower, standardized assurance levels tolerable
Latency not the overriding issue
Broad Interoperability is essential
Mostly local data used in applications

Electronic Business

Integrated Operations

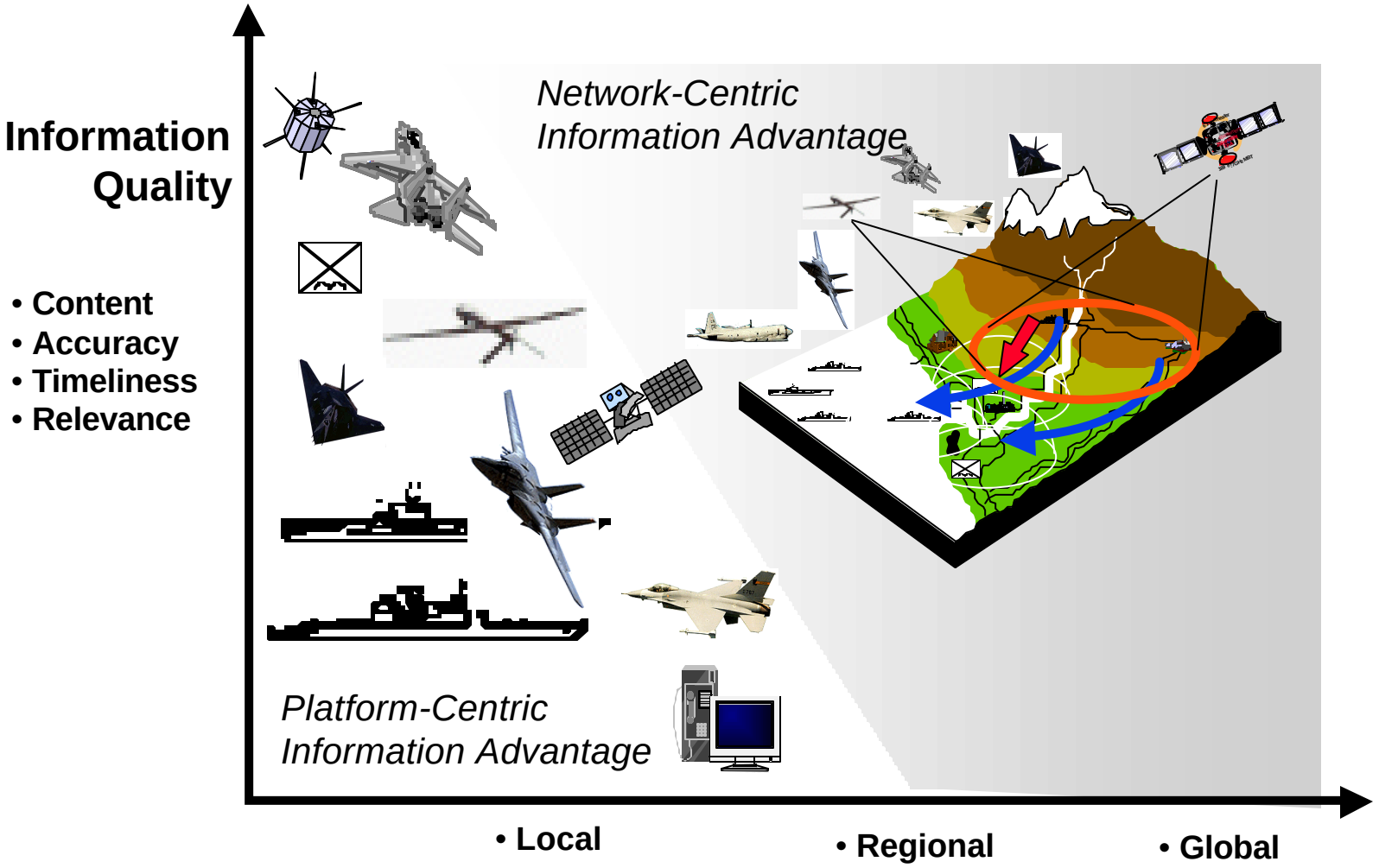
Enterprise Value derives from processes that must be reliably executed against strict timelines. Processes may be functional or cross functional but within a Community Of Interest (COI).

Higher levels of assurance necessary
Low tolerance of latency
Frequent access of shared services and data

Command & Control

DoD is a Federated Enterprise with some integrated Communities of Interest

Network Centric Operations
The Way Ahead



Transformation To Network Centric Warfare

Technologies

- Fiber Optic Transmission
- Unattended Aerial Vehicles (UAV)
- 3d Generation WIreless
- Public Key Infrastructure (PKI)
- Processor and Storage technologies
- Object Oriented Software

Operating Forces

- Joint AND Combined
- Smaller and More Agile
- Cross Functional and Data Centric
- ”Assured” vice “just in case” Operations
- Collaborative and Distributed
- Imagery Dependent

Suppliers

- Merged IT Service Providers
- Trans National Enterprises
- Functional Outsource

Emerging Threats

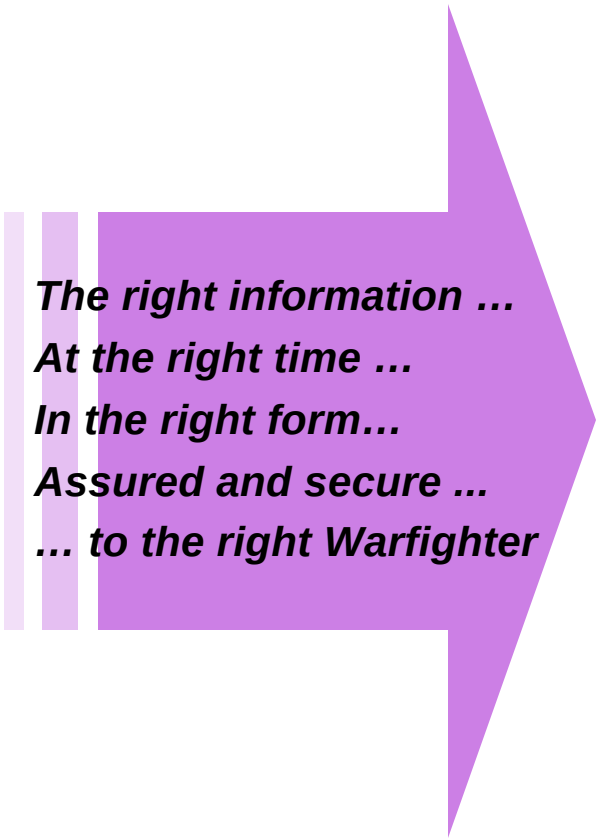
- Trans National Organizations
- State Sponsored Organizations
- Insider-outsider threat
- WMD threats

QDR Terms of Reference
Crisis & Conflict Scenarios

Necessary Transformation

From

Networks
Data
Personal Computing
Wired
Wireless
Defense in Depth



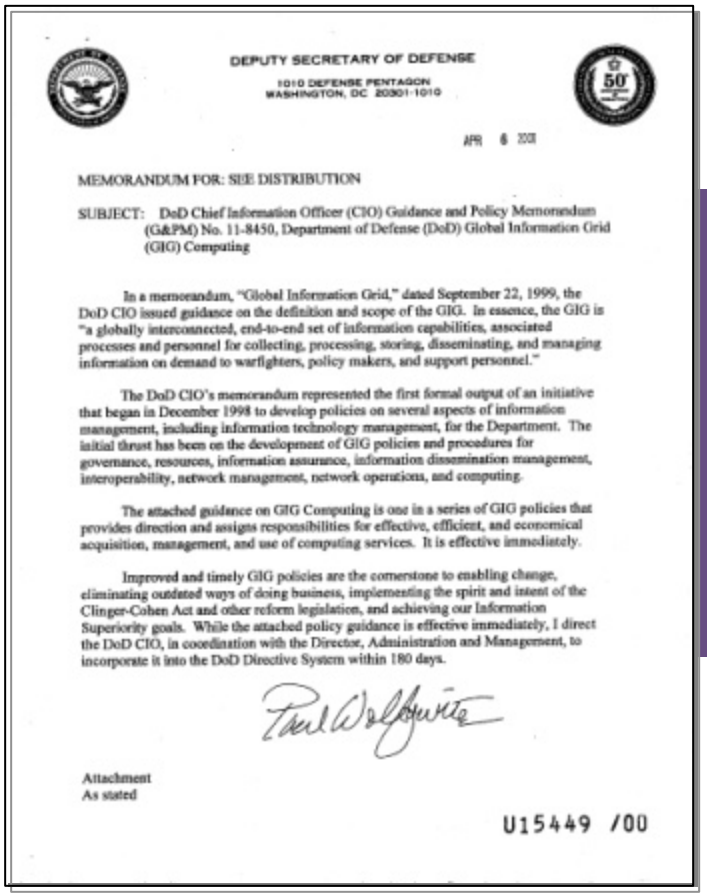
To

Worknets
Relationships
Interpersonal Computing
Wireless
Wired
Defense in Breadth

The Global Information Grid Defined

The GIG is the globally interconnected, end to end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policymakers, and support personnel

The Global Information Grid Defined



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

APR 6 2001

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: DoD Chief Information Officer (CIO) Guidance and Policy Memorandum (G&PM) No. 11-8450, Department of Defense (DoD) Global Information Grid (GIG) Computing

In a memorandum, "Global Information Grid," dated September 22, 1999, the DoD CIO issued guidance on the definition and scope of the GIG. In essence, the GIG is "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."

The DoD CIO's memorandum represented the first formal output of an initiative that began in December 1998 to develop policies on several aspects of information management, including information technology management, for the Department. The initial thrust has been on the development of GIG policies and procedures for governance, resources, information assurance, information dissemination management, interoperability, network management, network operations, and computing.

The attached guidance on GIG Computing is one in a series of GIG policies that provides direction and assigns responsibilities for effective, efficient, and economical acquisition, management, and use of computing services. It is effective immediately.

Improved and timely GIG policies are the cornerstone to enabling change, eliminating outdated ways of doing business, implementing the spirit and intent of the Clinger-Cohen Act and other reform legislation, and achieving our Information Superiority goals. While the attached policy guidance is effective immediately, I direct the DoD CIO, in coordination with the Director, Administration and Management, to incorporate it into the DoD Directive System within 180 days.

Attachment
As stated

U15449 /00

It includes

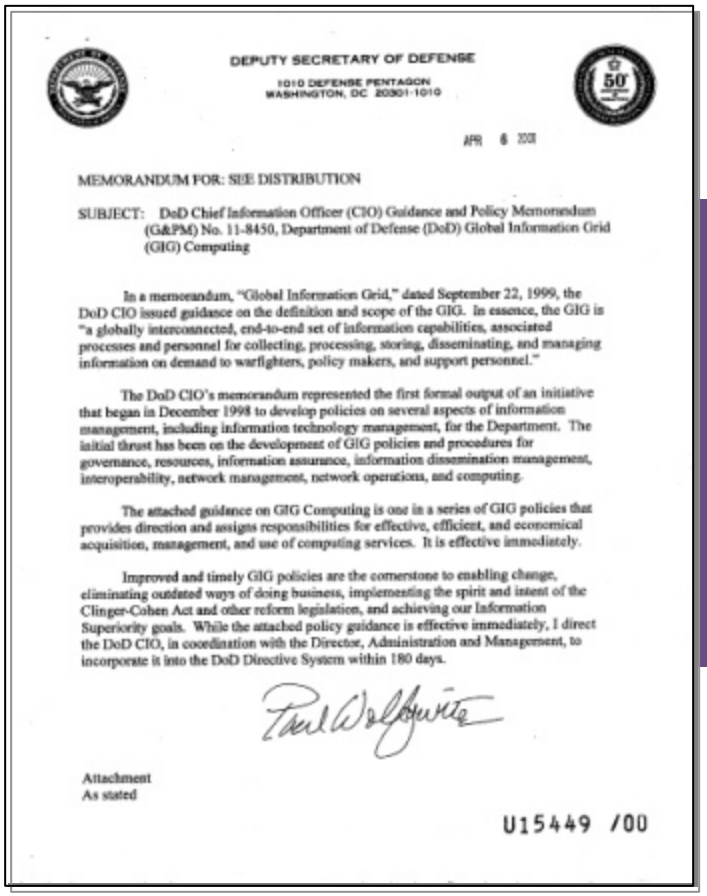
All owned or leased communications and computing systems and services (Including applications), data, security services, and other associated services necessary to achieve Information superiority

National Security Systems

Interfaces to coalition, allied, and non-DoD users and systems

The Global Information Grid Enables Network Centric Operations

The Global Information Grid Defined



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

APR 6 2001

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: DoD Chief Information Officer (CIO) Guidance and Policy Memorandum (G&PM) No. 11-8450, Department of Defense (DoD) Global Information Grid (GIG) Computing

In a memorandum, "Global Information Grid," dated September 22, 1999, the DoD CIO issued guidance on the definition and scope of the GIG. In essence, the GIG is "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."

The DoD CIO's memorandum represented the first formal output of an initiative that began in December 1998 to develop policies on several aspects of information management, including information technology management, for the Department. The initial thrust has been on the development of GIG policies and procedures for governance, resources, information assurance, information dissemination management, interoperability, network management, network operations, and computing.

The attached guidance on GIG Computing is one in a series of GIG policies that provides direction and assigns responsibilities for effective, efficient, and economical acquisition, management, and use of computing services. It is effective immediately.

Improved and timely GIG policies are the cornerstone to enabling change, eliminating outdated ways of doing business, implementing the spirit and intent of the Clinger-Cohen Act and other reform legislation, and achieving our Information Superiority goals. While the attached policy guidance is effective immediately, I direct the DoD CIO, in coordination with the Director, Administration and Management, to incorporate it into the DoD Directive System within 180 days.

Attachment
As stated

U15449 /00

Its part of the GIG if its networked and ...

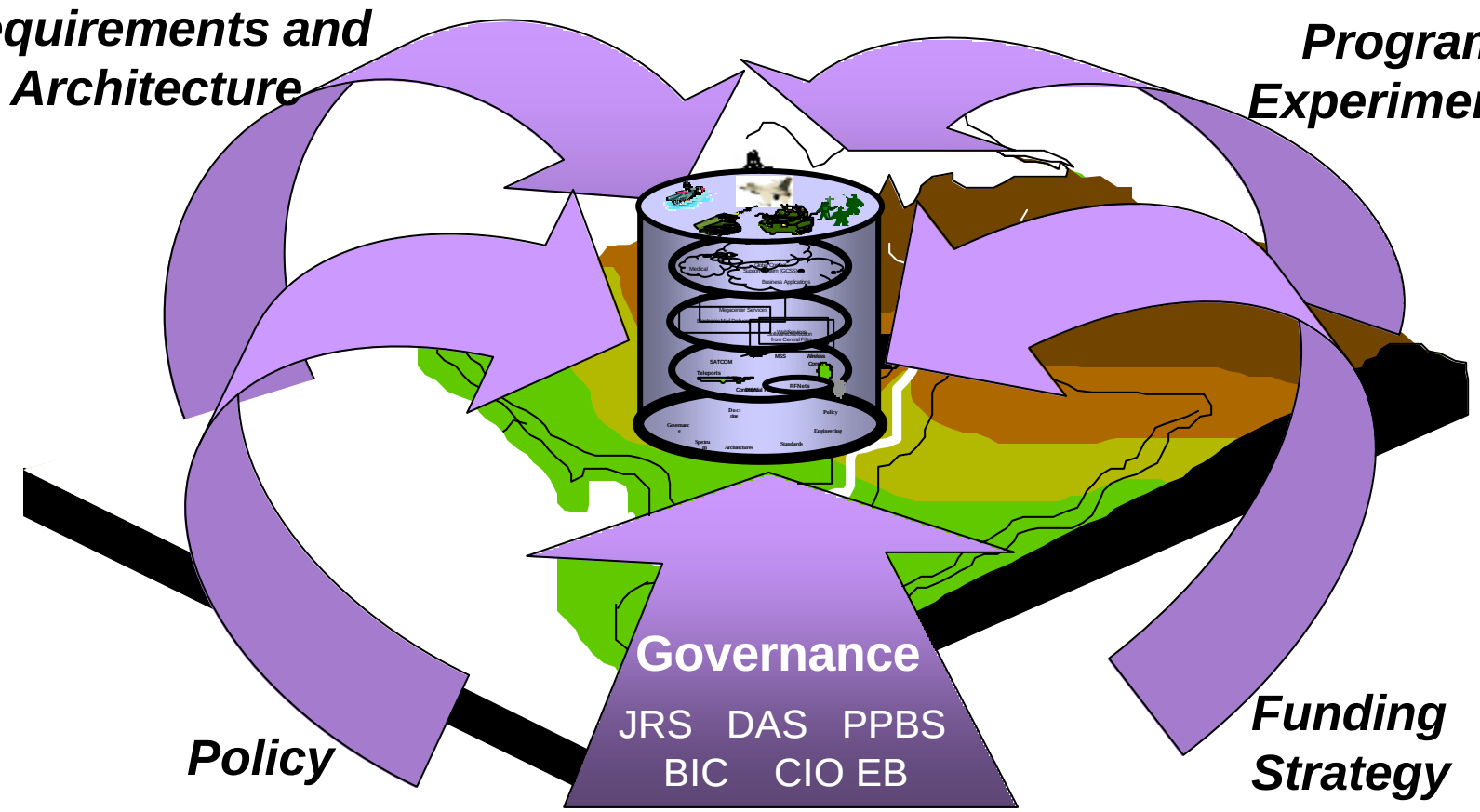
Transmits information to, receives information from, routes information among or interchanges information among other equipment, software and services …

Provides retention, organization, visualization, information assurance or disposition of data, information and/or knowledge received from or transmitted to other equipment, software and services

Processes data or information for use by other equipment, software and services

The Global Information Grid Enables Network Centric Operations

The GIG Campaign Plan



"Develop, maintain, and facilitate the implementation of

a sound and integrated information technology architecture *for the executive agency"*

(40 U.S.C. Section 1425)

GIG Implementation Tools - And Why They Matter to You

- **GIG Guidance and Policy Memoranda**
  - *establishes the direction and set the conditions for investment and implementation of networked information technology*
- **GIG Capstone Requirements Document**
  - *guides all DoD and Intelligence Community components in developing operational requirements documents (ORDS) for new systems and upgrading legacy systems*
  - *guides future IT investment to ensure interoperability*
- **GIG Architecture**
  - *establishes the Information Exchange Requirements for the Interoperability Key Performance Parameter*

GIG Guidance and Policy

http://www.c3i.osd.mil

- **DoD CIO G&PM 11-8450, DoD Global Information Grid (GIG) Computing(.pdf)**
- **DOD CIO G&PM 10-8460, 10-8460August 24, 2000, "GIG Network Operations" (.pdf)**
- **DOD CIO G&PM 7-8170, August 24, 2000, "GIG Information Management" (.pdf)**
- **DOD CIO G&PM 4-8460, August 24, 2000, "GIG Networks" (.pdf)**
- **DOD CIO Guidance and Policy Memorandum 6-8510 - Department of Defense Global Information Grid Information Assurance and Information Assurance Implementation Guide," signed June 16, 2000 (.pdf)**

- **DOD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001 - March 31, 2000 - Global Information Grid (.pdf)**

GIG Capstone Requirements Document

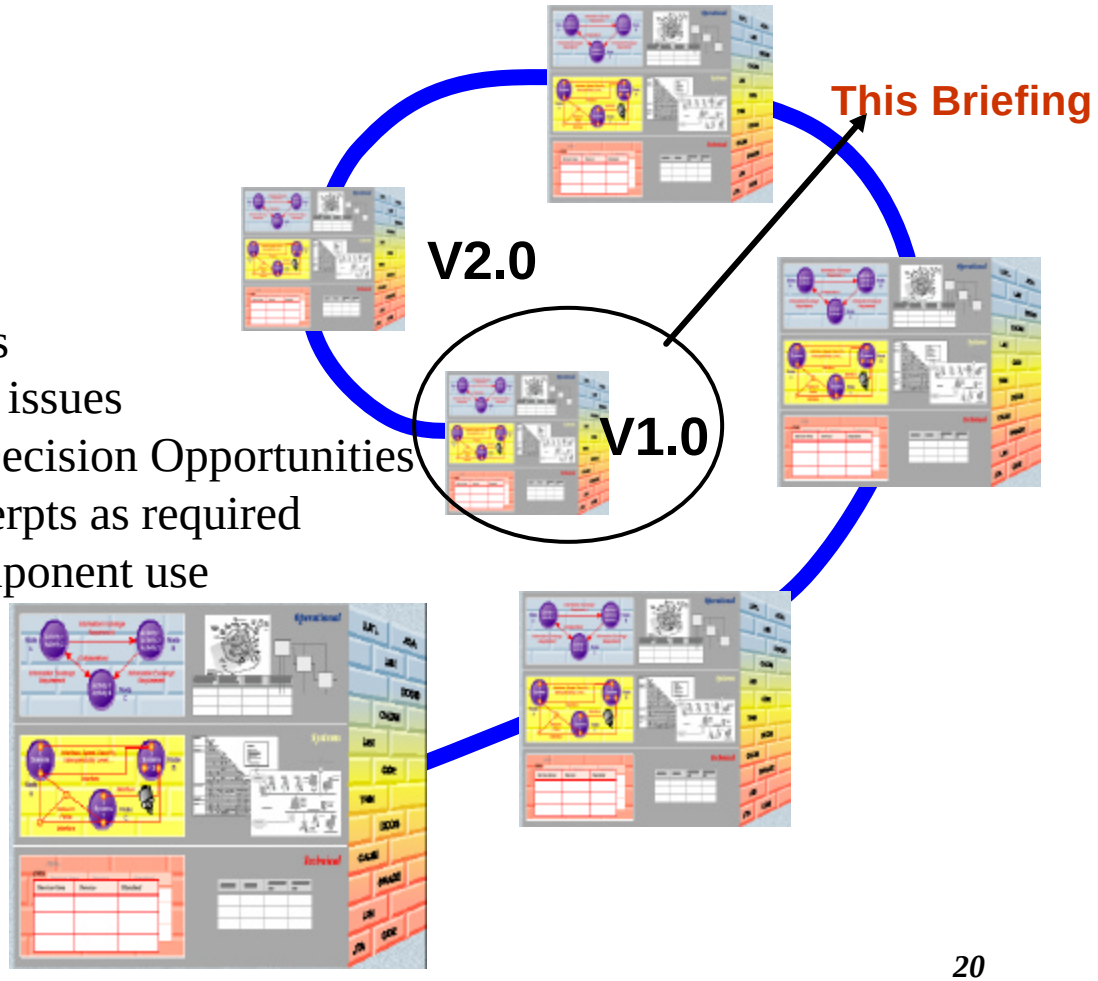
- **Developed by Joint Forces Command**
- **Approved by JROC 9 August 2001**
- **Establishes requirements and key performance parameters for all networked IT**
  - ***Processing***
  - ***Storage***
  - ***Transport***
  - ***Human-GIG Interface***
  - ***Information Assurance***
  - ***Network Management***
  - ***Information Dissemination***
- **Oversight tool for management of system of systems development**

GIG Architecture - Mandates

- **Clinger-Cohen Information Technology Management Reform Act (1996)**
  - ***develop, maintain and facilitate implementation of a sound and integrated technology architecture***
  - ***promote effective and efficient design and operation of all major information resources***
- **OMB Directive M96-17-A130**
  - ***describe business model and processes for IT investments***
  - ***provide architecture descriptors for IT investments***
- **Section 2223 US Code Title 10**
  - ***(DoD) "ensure that information technology and national security systems are interoperable with other relevant technology and national security systems"***

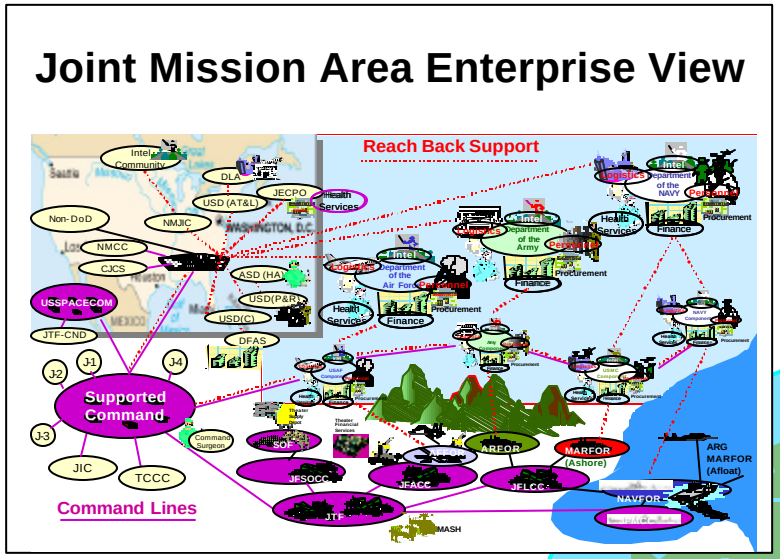
GIG Architecture

Spiral Development Approach

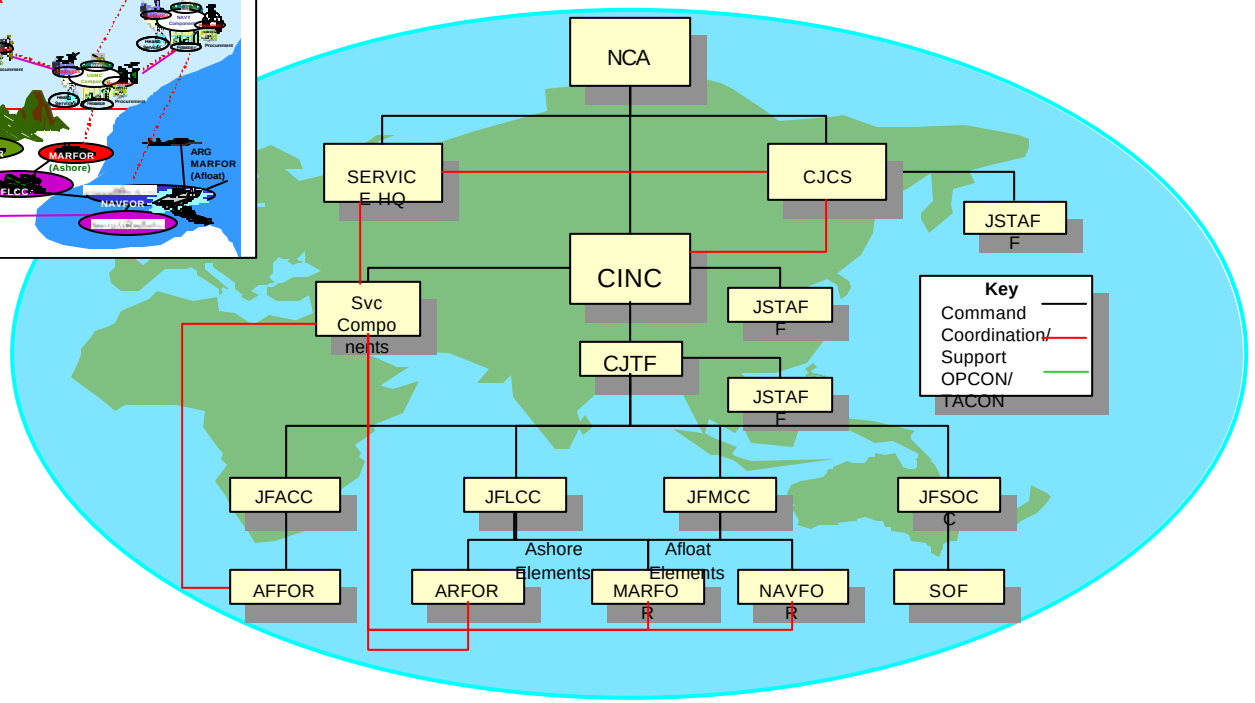


Major releases on 9-12 month centers
Tailored to address DoD DOTMLP-F issues
Synchronized with PPBS and Acq. Decision Opportunities
Classified SECRET w/UNCLAS excerpts as required
"Customized" where needed for Component use

GIG " Business Model"
Combined Joint Task Force Operations



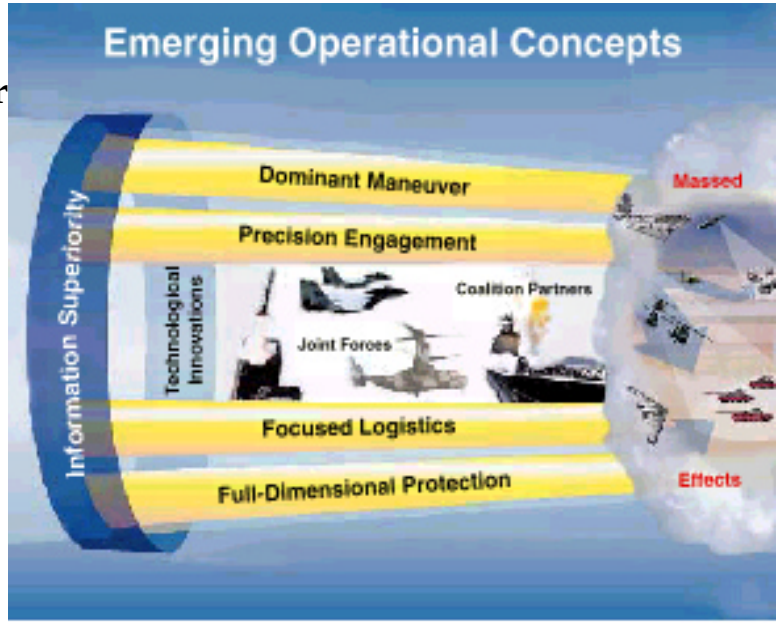
Combat and Sustainment Operations



Joint Mission Areas
Approved by Chairman/JCS
6 Sep 2000

JMAs (v. 2000)
"As Is"

JMA 1 Deployment and Redeployment
JMA 2 Movement and Maneuver
JMA 3 Employ Fires
JMA 4 Strategic Deterrence
JMA 5 Overseas Presence and Force Projection
JMA 6 MOOTW
JMA 7 Special Operations
JMA 8 Command and Control
JMA 9 Comm/Computer Environment
JMA 10 Information Operations
JMA 11 ISR
JMA 12 Logistics
JMA 13 Force Protection
JMA 14 Multinational Ops and Interagency Coordination



JMAs (v. 20XX)
"To Be"

1 Dominant Maneuver
2 Deployment/Redeployment
3 Precision Engagement
4 Strategic Deterrence
5 Overseas Presence and Force Projection
6 Special Operations
7 Joint Command and Control
8 Information Superiority
9 Focused Logistics
10 Full Dimensional Protection
11 Multinational Ops and Interagency Coordination

- Date of JMA transitions will vary
- Some may not transition IAW vision
- Some may be modified through experimentation/technology

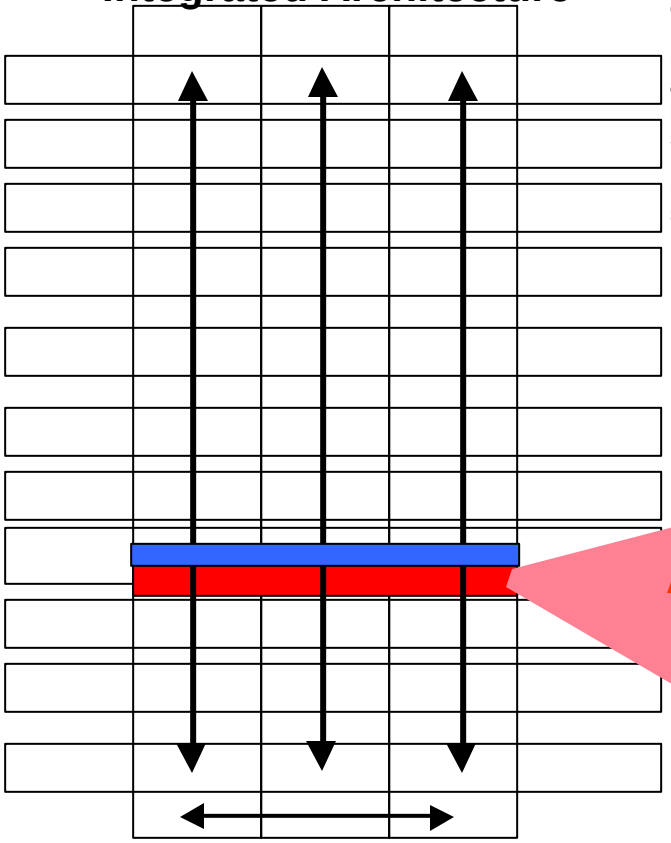
GIG Architecture

Networked IT

Global Information Grid Integrated Architecture

CJCS Approved objective Joint Mission Areas

1 Dominant Maneuver
2 Deployment/Redeployment
3 Precision Engagement
4 Strategic Deterrence
5 Overseas Presence and Force Projection
6 Special Operations
7 Joint Command and Control
8 Information Superiority
9 Focused Logistics
10 Full Dimensional Protection
11 Multinational Ops and Interagency Coordination

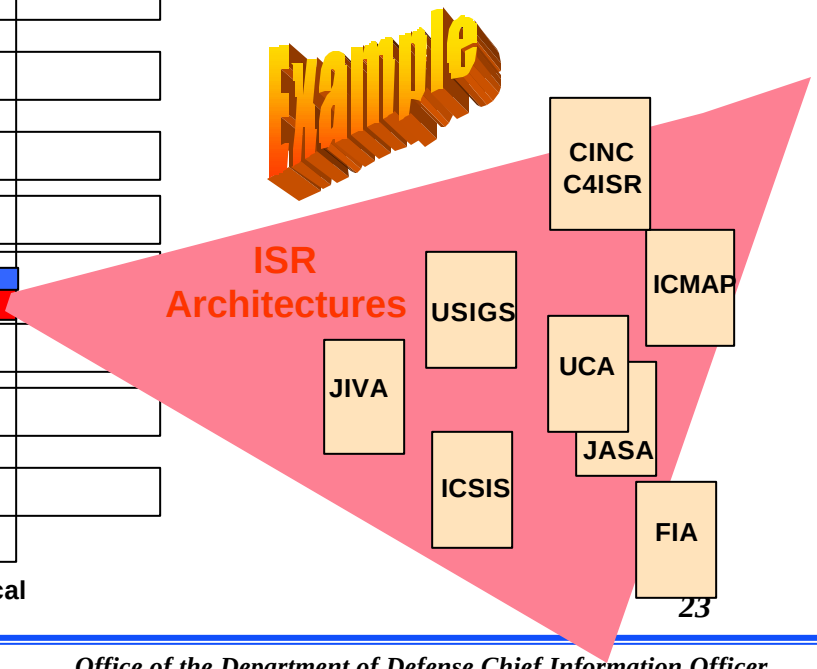


Operational View | Systems View | Technical View

Transmits information to, receives information from, routes information among or interchanges information among other equipment, software and services …

Provides retention, organization, visualization, information assurance or disposition of data, information and/or knowledge received from or transmitted to other equipment, software and services

Processes data or information for use by other equipment, software and services



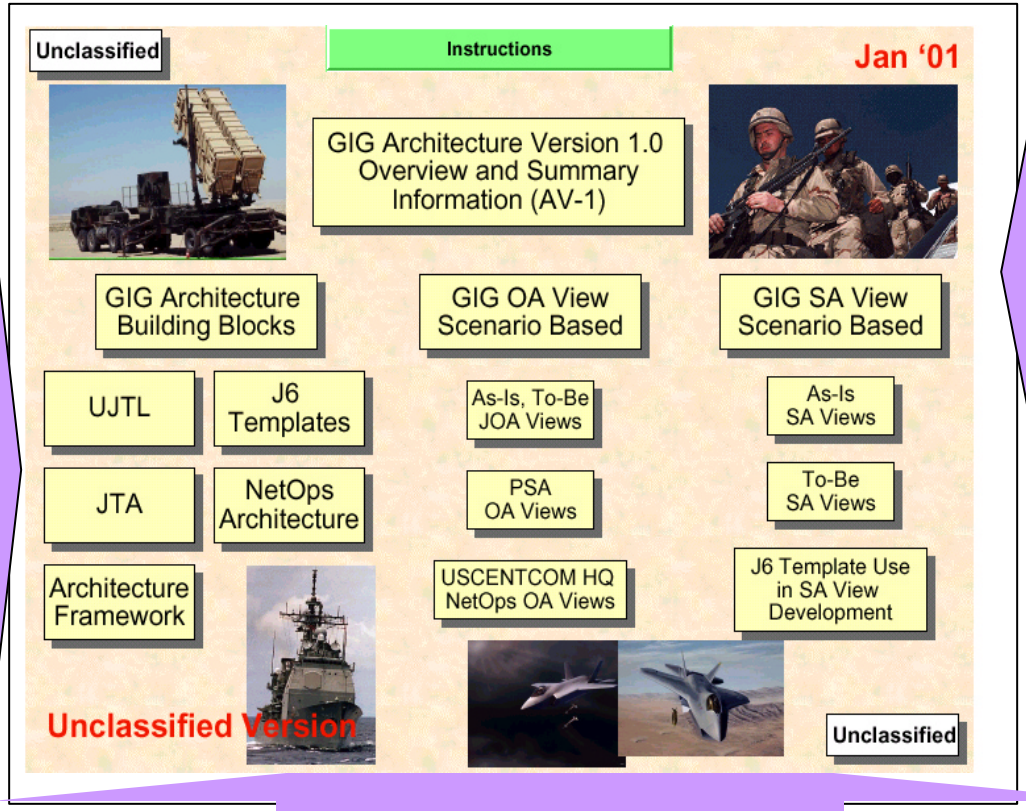
Version 1.0 Contents

Joint Operational Architecture V1.0

CINC Architecture Products

"Business" Architecture Data

P&R HA
Log Fin
Intell



Joint Technical Architecture

"As-Is" - 2003

"To Be" - 2010

Threat to the Global Information Grid

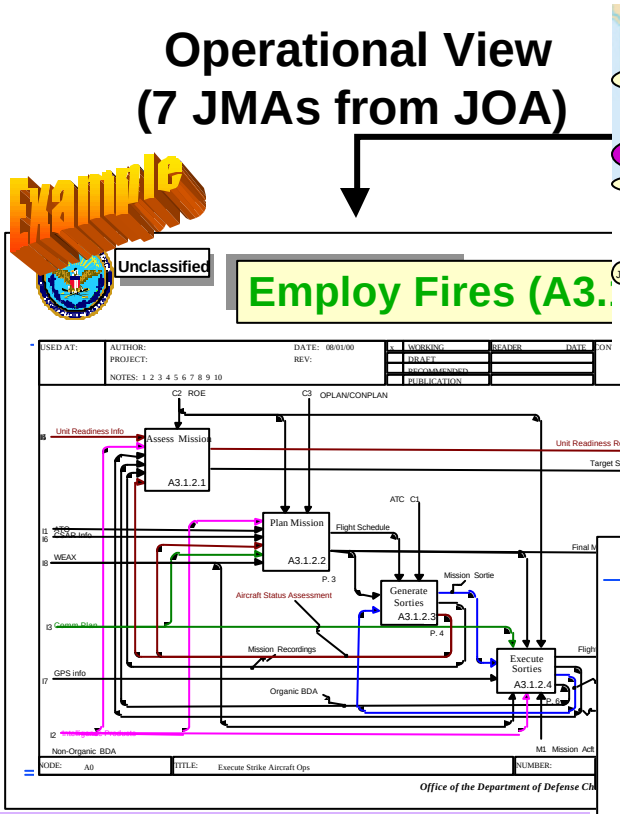
SWA Operational Scenario

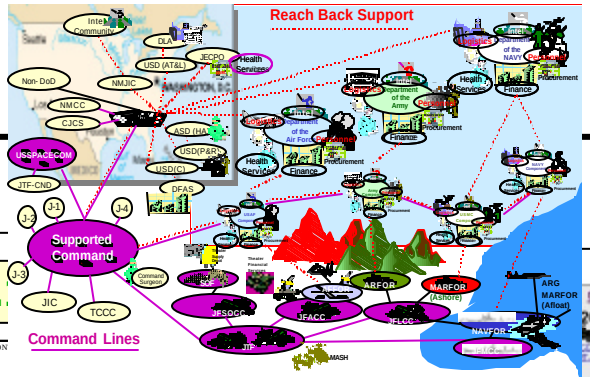
Timelines Joint Forces Triggers

GIG Architecture V1.0 Coverage

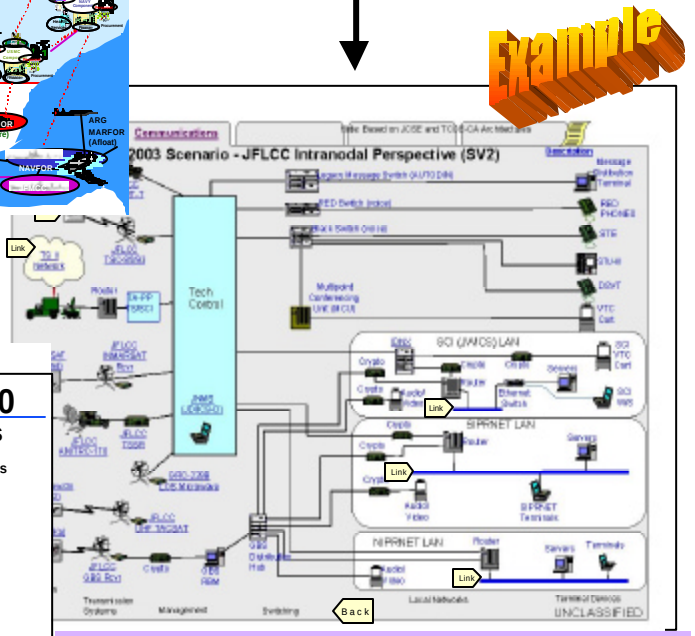
C/JTF Joint Mission Area Enterprise

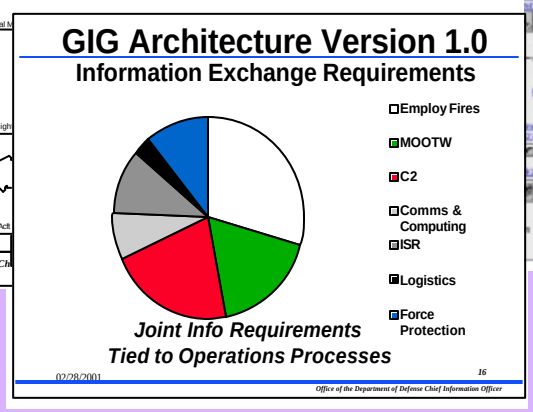
Operational View (7 JMAs from JOA)





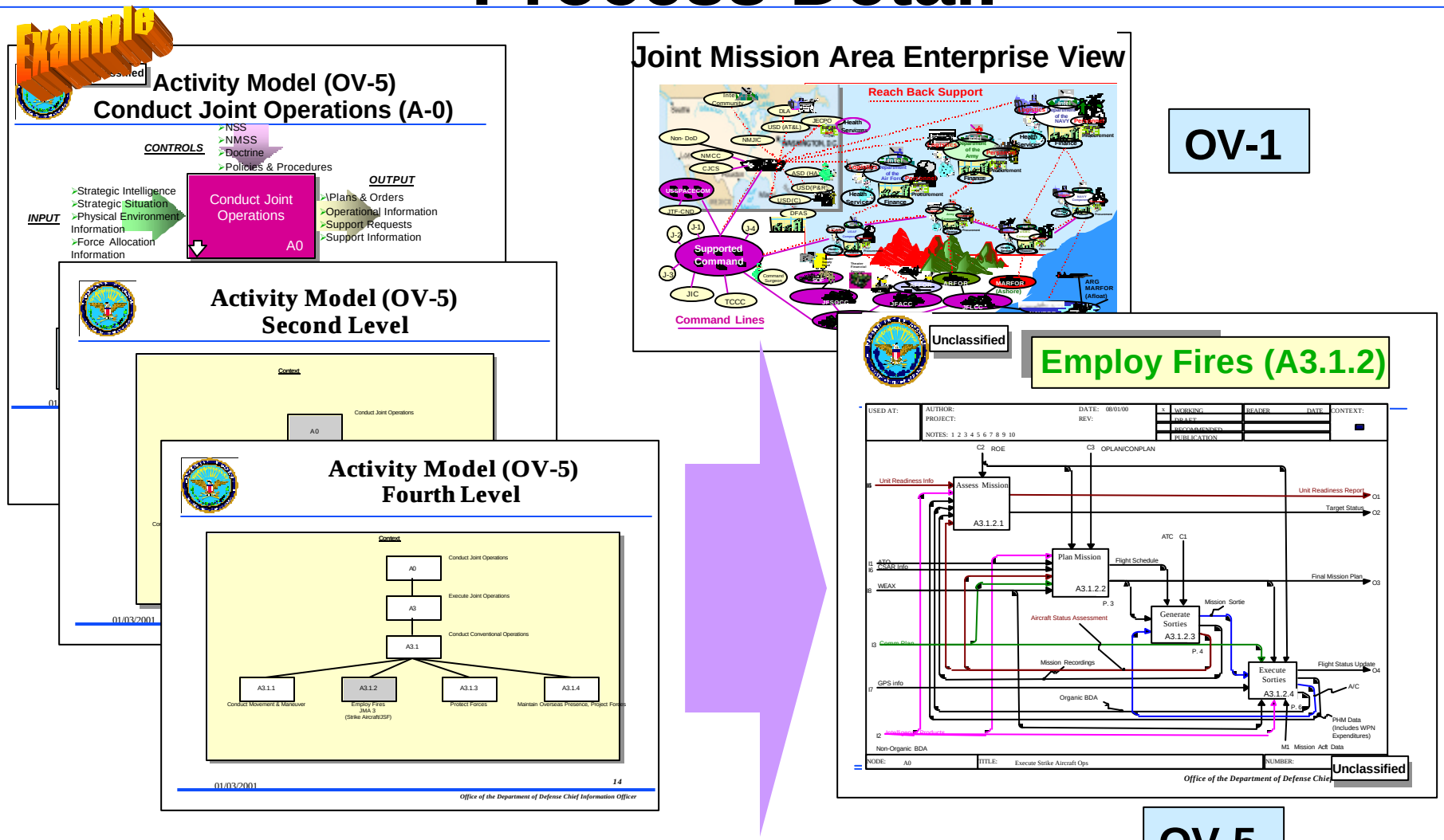
System View



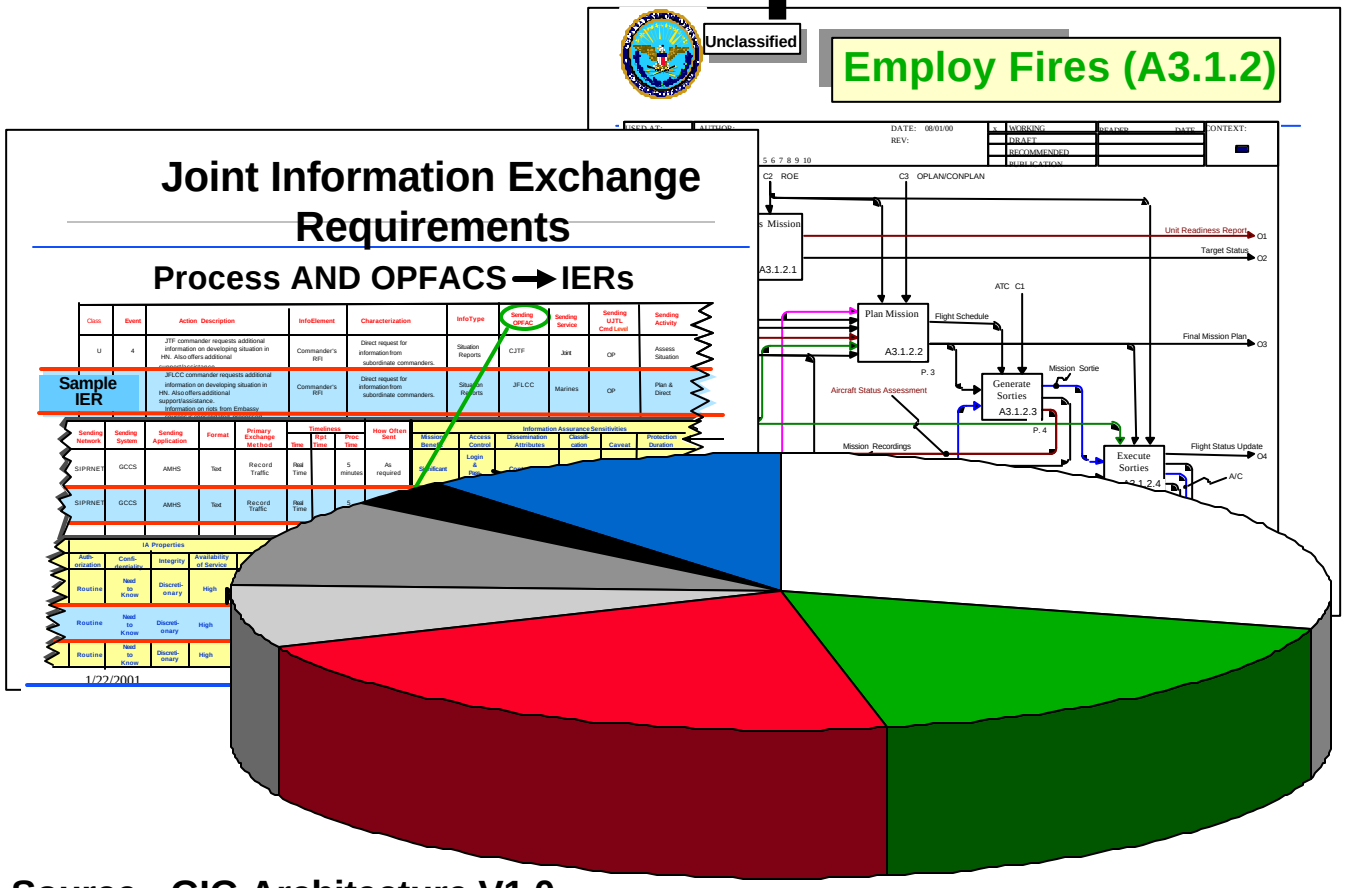


Modifications to the Joint Technical Architecture

Operational View Process Detail



Joint Information Exchange Requirements



Source: GIG Architecture V1.0

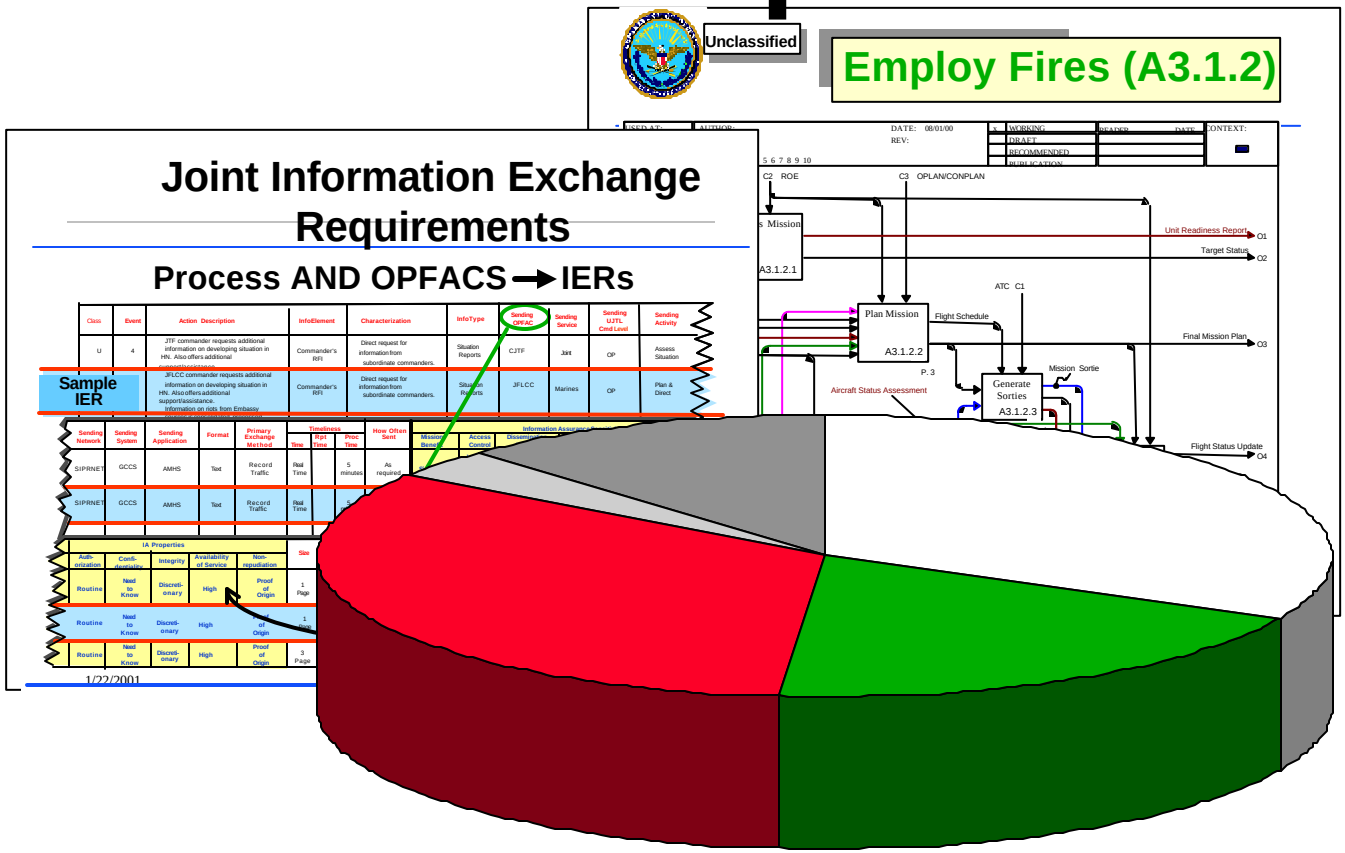
Over 3600 Joint Information Requirements are now tied to operations processes

"As Is" Joint Mission Area

- Employ Fires
- MOOTW
- C2
- Comms & Computing
- ISR
- Logistics
- Force Protection

09/23/2002

Joint Information Exchange Requirements



"To Be" Joint Mission Area

- Precision Engagement
- Overseas Presence & Force Projection
- Information Superiority
- Focussed Logistics
- Full Dimension Protection

Source: GIG Architecture V1.0

Over 3600 Joint Information Requirements are now tied to operations processes

GIG Threat Baseline

Kinetic Threat to Data Center Facilities

- Covertly emplaced explosives
- Projectile delivered explosives

Chemical/Biological Threat to Data Center Personnel

- Aerosol delivered persistent chemical/biological agents
- Insider delivered biological agent

Information Threat to Networks and Computing Systems

- Disclosure of operations/business details
- Deception causing loss of confidence in a system
- Denial of system resources to support an operation/business
- Usurpation of system resources for criminal purposes

The Global Information Grid will face an asymmetric and non-traditional threat environment

Challenges To Success

DoD Process	Challenge
Requirements	Interoperability KKPs are in early stage of use Role of architectures in developing ORDs are embryonic IT deployment will change the requirements baseline
Acquisition	Key aspects of the acquisition process are vertically configured Cross-system issues do not naturally surface to decision makers Compliance with interoperability policy is disincentivized
Prog. & Budget	Current PPBS practice does not recognize the interdependencies that are needed for network centric operations
Info Resources Mgmt	Information Assurance could evolve into another stovepipe Security is not viewed as a basic data attribute The content of the "Warfighters' infosphere" is very spotty

Implementing the GIG given these challenges will require committed and active leadership